Journal of Iranian Social Development Studies (JISDS)
2024 (Autumn), Vol. 16, No. 4

Explaining the concept and scope of political geography of cyber space

Afshin Motaghi [1]
Associate Professor of Political Geography, Faculty of Geographical Sciences, Kharazmi University, Tehran, Iran (Corresponding Author)
Arash Ghorbani Sepehr [2]
Postdoctoral Researcher of Political Geography, Faculty of Geographical Sciences, Khwarazmi University, Tehran, Iran
Parisa Ghorbani Sepehr [3]
Doctoral student of Political Geography, Faculty of Geographical Sciences, Khwarazmi University, Tehran, Iran

Abstract: *Cyber space cannot be fully understood without understanding the role of space. Cyber space is a complex, decentralized and dynamic space with many components and diverse features. Therefore, the field of cyberspace geography is relatively new and much more variable than other environments. But what initially seemed like the Internet was supposed to end geography; But this was not the case and the cyber space was used as a complement to the geographical space. Therefore, in the current era, each of the geographical sciences seeks to understand the dimensions of cyber space, among which political geography is a science that discusses and examines the concepts of cyber space. Based on this, the current research is based on the method of content analysis and the use of library data in order to answer the question, what is the conceptualization and scope of the political geography of cyber space? The findings show that cyberspace and related technologies are one of the most important sources of power in the third millennium. Therefore, cyberspace is considered one of the geopolitical power generating components for countries; So that today powerful countries influence other countries by using the capacities of cyber space. On this basis, the political geography of cyberspace is formed from human action with a political dimension on cyberspace. Therefore, political geographers can study the cyberspace and present plans to the statesmen to organize this space in line with [its better management].*

Keywords*: Conceptology, space, cyberspace, political geography, political geography of cyberspace.*

[1] Email: a.mottaghi@khu.ac.ir (Corresponding Author)
[2] Email: ar.ghorbanisepehr@mail.um.ac.ir
[3] Email: Parisa.ghorbanisepehr98@gmail.com

مجله مطالعات توسعه اجتماعی ایران، سال شانزدهم/ شماره چهارم/ پاییز ۱۴۰۳
Journal of Iranian Social Development Studies 2024 (Autumn), Vol. 16, No. 4

تبیین مفهوم و قلمرو جغرافیای سیاسی فضای سایبر

افشین متقی[1]*، آرش قربانی سپهر[2]، پریسا قربانی سپهر[3]

تاریخ دریافت مقاله: ۱۴۰۲/۱۲/۲۱ تاریخ پذیرش مقاله: ۱۴۰۳/۰۲/۲۹

چکیده
فضای سایبر را نمی‌توان بدون درک نقش فضا به طور کامل درک کرد. فضای سایبر یک فضای پیچیده، غیرمتمرکز و پویا با اجزای متعدد و ویژگی‌های متنوع است. از این‌رو، حوزۀ جغرافیای فضای سایبر نسبتاً جدید است و نسبت به سایر محیط‌ها بسیار تغییرپذیرتر است. اما آن چیز که در ابتدا به نظر می‌رسید اینترنت قرار بود به جغرافیا پایان دهد؛ اما اینگونه نبود و فضای سایبر به عنوان مکمل فضای جغرافیایی به کار گرفته شد. لذا در عصر حاضر هر یک از علوم جغرافیایی در پی شناخت ابعاد فضای سایبر هستند که در این بین جغرافیای سیاسی دانشی است که مفاهیم فضای سایبر را مورد بحث و بررسی قرار می‌دهد. بر این مبنا، پژوهش حاضر مبتنی بر روش تحلیل محتوا و استفاده از داده‌های کتابخانه‌ای در پی پاسخ به این سؤال است که مفهوم‌سازی و قلمرو جغرافیای سیاسی فضای سایبر چیست؟ یافته‌ها گویای آن است که فضای سایبر و فناوری‌های مرتبط یکی از مهم‌ترین منابع قدرت در هزارۀ سوم است. از این‌رو، فضای سایبر یکی از مؤلفه‌های قدرت‌زای ژئوپلیتیکی برای کشورها محسوب می‌شود؛ به‌طوری که امروزه کشورهای قدرتمند با بهره‌گیری از ظرفیت‌های فضای سایبر بر دیگر کشورها تأثیر می‌گذارند. بر این بنیاد، جغرافیای سیاسی فضای سایبر، از کُنش انسان با بُعد سیاسی بر فضای سایبر شکل می‌گیرد. بنابراین، جغرافی‌سیاسی‌دانان می‌توانند فضای سایبر را مطالعه و برنامه‌هایی را جهت به سامان شدن این فضا به دولتمردان در راستای [ادارۀ بهتر آن] ارائه دهند.

واژگان کلیدی: مفهوم‌شناسی، فضا، فضای سایبر، جغرافیای سیاسی، جغرافیای سیاسی فضای سایبر

۱. مقدمه
جغرافیای سیاسی تحت تأثیر نحوۀ تعامل قدرت و فضا قرار گرفته است. کشورها بر اساس سرزمینی که قادر به کنترل آن هستند، همانطور که توسط مرزهایشان تعریف شده است، تعیین می‌شوند. قدرت آنها در یک موقعیت نظری مبتنی نیست بلکه به فضای جغرافیایی متصل است. قدرت یک دولت فقط تا حد یک خط خیالی است که در یک جسم فیزیکی جامد ساخته شده است. بازیگران سیاسی، چه مردان و چه دولت‌ها، به یک نظام جغرافیایی احترام گذاشته و آن را به هوا و دریا نیز گسترش داده‌اند.

[1] دانشیار جغرافیای سیاسی، دانشکدۀ علوم جغرافیایی، دانشگاه خوارزمی، تهران، ایران (نویسنده مسئول).
(E mail: a.mottaghi@khu.ac.ir)
[2] پژوهشگر پسادکتری جغرافیای سیاسی، دانشکدۀ علوم جغرافیایی، دانشگاه خوارزمی، تهران، ایران.
(E mail: ar.ghorbanisepehr@mail.um.ac.ir)
[3] دانشجوی دکتری جغرافیای سیاسی، دانشکدۀ علوم جغرافیایی، دانشگاه خوارزمی، تهران، ایران.
(E mail: Parisa.ghorbanisepehr98@gmail.com)

فضاهای کالبدی از زمان تأسیس دولت مدرن با جوهر قدرت مرتبط بوده است. با این حال، این بحث وجود دارد که آیا این چارچوب می‌تواند در عصر جدید فناوری ادامه یابد یا خیر (Sheldon, 2014: 286). بیش از دو دهه، فضای سایبر نقش مهمی در ارتباطات جهانی ایفا کرده و به طور فزاینده‌ای در زندگی مردم در سراسر جهان ادغام شده است (Tan et al., 2021: 673). فضای سایبر یک شبکهٔ جهانی گسترده ایجاد کرده است که سالانه میلیاردها دلار برای اقتصاد جهانی درآمد تولید می‌کند (Judge et al., 2021). در حال حاضر بیشتر فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و دولتی کشورها در تمامی سطوح اعم از افراد، سازمان‌های مردم نهاد و نهادهای دولتی در این فضا انجام می‌شود (Aghajani & Ghadimi, 2018: 220). به عبارت دیگر، جنبه‌های مختلف زندگی ملت‌ها به معنای واقعی کلمه با این فضا در هم آمیخته شده است و هرگونه بی‌ثباتی، ناامنی و چالش در این فضا مستقیماً بر جنبه‌های مختلف زندگی آنان در کشورها تأثیر می‌گذارد (Li et al., 2020). با این وجود فضای سایبر چالش‌های امنیتی جدیدی را برای دولت‌ها ایجاد کرده است (Thomson, 2015: 50). ظهور رسانه‌های اجتماعی فراگیر در جهان پویایی‌های انسانی در فضای فیزیکی را کمرنگ ساخته و این پویایی در فضای مصنوعی- سایبری گسترش یافته است و بر کشورها و ملت‌ها تأثیر می‌گذارد (Li, Zhao, He, Mansourian, & Axhausen, 2021: 95).

بنابراین می‌توان با توجه به تأثیرات پراهمیت فضای سایبر بر کشورها، نقش و جایگاه آن را به عنوان عاملی مهم در نظر داشت. زیرا که با مقبولیت جهانی اینترنت و فضای سایبر، مفهوم مکان از یک دیدگاه مشخصی کنار گذاشته شده است، ارتباطات بین قاره‌ای و انتقال اطلاعات با یک اشاره بر صفحه کلید رایانه‌ها امکان‌پذیر می‌باشد (قربانی سپهر و انصاری، ۲:۱۳۹۷).

بر این بنیاد، فضا یک مقولهٔ بسیار عام است. فضا تمام جهان هستی را در برمی‌گیرد و ما را در تمام طول زندگی احاطه کرده است. هر کاری که انسان انجام می‌دهد، دارای یک جنبهٔ فضایی نیز است، به عبارتی هر عملی که انجام می‌شود، احتیاج به فضا دارد، در واقع فضا عرصهٔ مانور انسان برای حیات و زندگی است. از این‌رو، با نفوذ گستردهٔ رسانه‌های جمعی به ویژه رسانه‌های اجتماعی، شبکه‌های اجتماعی مجازی و ابزارهای پیام‌رسان موبایلی، ابعاد مختلف فضای زندگی انسان را به طور عام و کنشگران سیاسی آن به طور خاص هر چه بیشتر در محدوده و تحت تأثیر این پدیده‌های فناورانهٔ نوظهور در عصر اطلاعات و جامعهٔ اطلاعاتی قرار داده است. این گسترش فضای سایبر در دوران کنونی بخش جدایی‌ناپذیر زندگی انسان‌ها می‌باشد و در طول شبانه روز از محتوای اجتماعی، سیاسی، اقتصادی و آموزشی آن استفاده می‌کنند. در زندگی انسان امروز و در پرتو نقش‌آفرینی گستردهٔ رسانه‌های اجتماعی مبتنی بر وب، عرصهٔ سیاست‌ورزی رسمی بیش از پیش، از نهان هزار توی مکان‌های خصوصی به مکان‌های عمومی نقل مکان کرده و تمام افراد جامعه را درگیر خود، ساخته است (انصاری و همکاران، ۱۸۹:۱۳۹۷). با توجه به ظرفیت فضای سایبر در جهان دیجیتال، هر یک از علوم به نحوی در گسترش و کنترل آن نقش دارند که در این بین جغرافیای سیاسی به عنوان علمی که در فضای فیزیکی به بررسی مفاهیمی همچون (مرز، ملت، حکومت، دولت، سرزمین، امنیت و...) می‌پردازد، نیاز است همین مفاهیم را در فضای سایبر به منظور مدیریت این فضا مفهوم‌سازی نماید تا حکومت‌ها و دولت‌ها بهتر بتوانند این فضا را به سامان کنند؛ زیرا امروزه کنشگری در فضای سایبر بیش از فضای فیزیکی است و فضای سایبر بر فضای فیزیکی تأثیر می‌گذارد. بر این مبنا، پژوهش حاضر در پی پاسخ به این پرسش است که چگونه می‌توان مفهوم‌سازی و قلمروسازی درست از جغرافیای سیاسی فضای سایبر ارائه داد؟

۲. مفهوم‌شناسی نظری

- فضا

انسان و فضا از کانونی‌ترین مفاهمی دانش جغرافیایی به شمار می‌روند (رحیمی، ۹۲:۱۳۹۵). در جغرافیا نیز مفهوم فضا، پدیدهٔ حاصل از رابطهٔ انسان و محیط و بُن‌مایهٔ اصلی این علم شناخته می‌شود (Soja, 1990: 120). فضا، به شکل‌های مختلف، موضوع

کلیدی جغرافیاست. فضا احتمالاً پُراستنادترین واژه‌ای است که به جغرافیا هویت و کانونی وحدت‌بخش داده است. با این اوصاف، تلاش برای بازتعریف جغرافیا به مثابه علم فضایی به این واژه جایگاه می‌بخشد. بنابراین دانشوران جغرافیای انسانی و طبیعی هر دو از این واژه مرتباً استفاده می‌کنند، اما از تعریف آن عاجز مانده‌اند و برای بسیاری آنچنان متنوع به نظر می‌رسد که فاقد هر گونه صراحت سودمندی است (Kitchin & Thrift, 2009). فضا، نظامی باز و پویا از کنش متقابل میان مکان‌هاست. بدون ادراک مفهوم «فضا» آن فهم جغرافیا با کاستی همراه خواهد بود (حافظ‌نیا و کاویانی‌راد، ۲۱۳:۱۳۹۳). فضا تولید می‌شود و سازمان می‌یابد (Brunet,1996:123). از این‌رو، فضا یکی از مفاهیمی است که بیشترین ابهام برای تبیین و مرزبندی آن وجود دارد و همین امر گاه آن را به سوی نوعی درک ناپذیری سوق می‌دهد. دلیل آن است که باید فضا را باید بیش از هر چیز به مثابه مکانی «خالی» و «تهی» در نظر گرفت، جایی که هیچ چیز را در خود جای نمی‌دهد در عین حال، فضا را می‌توان و باید از خلال قابلیت (پتانسیل‌های) حرکت و یا عدم چنین قابلیت‌هایی و چگونگی شکل گرفتن حرکت، جریان و سکون آن درک کرد. هر کالبد با ورود به درون یک فضا به نوعی وادار به اطاعت و تبعیت از آن می‌شود و فضا به نوعی آن را به تملک خود درمی‌آورد، تملکی که می‌تواند (و اغلب نیز چنین است) به شکلی دوسویه آید و پیامدهای خاصی را نیز در خود دارد (Jedrej, 2000: 547). بر این پایه، فضا در ذات خود ماهیتی پیوسته و یکپارچه دارد؛ و این ماهیت در غالب سامانه‌های منطقی، به اجزایی ناپیوسته و از هم گسسته تقلیل می‌یابد (Hillier & Hanson, 1984: 33). لوفور فضا را یک تمامیت تاریخی و یک تولید اجتماعی می‌داند که از یک سو تجربهٔ تاریخی و از سوی دیگر تجربهٔ زندگی روزمرهٔ ماست (منوچهری میاندوآب و رهنمایی، ۸۶:۱۳۹۸). به هر روی، فضا گستره‌ای پیوسته است که پدیده‌ها، شیءها و اندیشه‌ها و اندیشنده‌ها در آن قرار می‌گیرند (قربانی سپهر، ۳۸۵:۱۳۹۷) و فضا در درک تغییراتی که فضای سایبر برانگیخته است، نقش اساسی دارد. بر این بنیان اندیشه‌ها و اندیشنده‌ها در شکل‌گیری و گسترش فضای سایبر بسیار مؤثر بوده‌اند که در ادامه به آن می‌پردازیم.

- فضای سایبر

جغرافیدانان با تأکید بر فضا اشاره می‌کنند که فضا و مکان در موقعیت مناسبی قرار دارند که به طور قابل توجهی به مطالعات فضای سایبر اضافه می‌شوند؛ بنابراین، فضای سایبر را نمی‌توان بدون درک نقش فضا به طور کامل درک کرد (Kitchin, 1997: 149). فضای سایبر یک فضای پیچیده، غیرمتمرکز و پویا با اجزای متعدد و ویژگی‌های متنوع است. این فضا از شبکه‌های مستقلی تشکیل شده است که با استفاده از پروتکل اینترنت (IP) و سوئیچینگ بسته با یکدیگر ارتباط برقرار می‌کنند (Park, 2005: 322). با توجه به ساختار پراکندهٔ فضای سایبر، ارزیابی هر عنصری از آن در مقیاس جهانی چالش‌برانگیز است. در آغاز سال ۲۰۲۱، تعداد شبکه‌های مستقل منحصربه‌فرد در سیستم مسیریابی اینترنت به ۹۹،۳۷۸ رسید (Maigron, 2020). در همین سال تعداد کاربران اینترنت ۷،۶ درصد افزایش یافت و در حال حاضر ۶۰ درصد از جمعیت جهان آنلاین هستند. حجم داده‌های ایجاد شده در هر روز تقریباً ۱،۱۴۵ تریلیون مگابایت است. در شبکه، داده‌ها به بسته‌ها تقسیم می‌شوند. یک بسته، بخش کوچکی از یک پیام بزرگتر است که به دستگاه‌هایی مانند تلفن‌های هوشمند و رایانه‌ها هدایت می‌شود و حاوی اطلاعات کنترل و کاربر است (Stallings & Slyke, 2201). از این‌رو، دیجیتالی شدن بر اساس فرآیند همه منظورهٔ دنیای فضای سایبر است که با ظهور علم کامپیوتر در حدود دههٔ ۱۹۵۰ آغاز شده است (Autio, 2017; Rijswijk et al., 2021: 83). از طریق فضای سایبر، داده‌ها را می‌توان از زندگی روزمرهٔ افراد، تعاملات، فعالیت‌های تجاری یا اشیاء فیزیکی تولید کرد و سپس انتقال داد (van Dijck, 2014: 200; Mejias and Couldry, 2019).

برای درک کامل ظرایف اخلاقی- اجتماعی و مفاهیم عمیق‌تر فضای سایبر باید به طور گسترده‌تر به عنوان فرآیندی در نظر گرفته شود که طی آن طیف وسیع‌تری از عناصر دیجیتالی به تدریج توسط سیستم‌های فیزیکی- اجتماعی استفاده شده و بر آنها

تأثیر می‌گذارد (Bronson, 2019: 110; Rijswijk et al., 2021; Vial, 2019: 122). این درک گسترده‌تر، فضای سایبر را به سمت ابعاد و ویژگی‌های دیگر باز می‌کند، از فناوری‌های دیجیتال گرفته تا زیرساخت‌های داده، اتصال، استراتژی‌های دیجیتال، وظایف/ مهارت‌های دیجیتال و... (Prause et al., 2021: 71; Rose et al., 2021: 307; Sparrow & Howard, 2021: 825). با این حال، در آغاز دهۀ ۱۹۹۰، رشد خیره کنندۀ ارتباطات رها شده از محدودیت‌های زمانی و مکانی، نوید دموکراتیک کردن و آرام کردن جهان را از طریق گسترش ایده‌ها و ارزش‌های دموکراتیک داد. ظهور فضای سایبری که از پیوند شبکه‌ها به وجود آمده بود، حتی ظهور یک «دهکدۀ جهانی» را در تصویر رؤیایی که شصت سال قبل توسط مارشال مک‌لوهان (۱۹۶۴) صورت‌بندی شده بود، نشان داد. از نظر تاریخی، گسترش شبکه‌های ارتباطی منجر به آرمان‌شهر جهانی بهتر شد (Douzet, 2014: 11). فضای سایبر به عنوان فضایی برای همه تبلیغ می‌شود. با این حال، واضح است که استفاده از فضای سایبری در امتداد تقسیمات سنتی فضایی و اجتماعی تکه تکه شده است و برای عموم قابل دسترسی نیست. در واقع، به دور از ایجاد یک جامعۀ برابرتر، برخی از مفسران پیشنهاد کرده‌اند که فضای سایبر نابرابری‌های جدیدی را تقویت کرده و ایجاد می‌کند و جهانی نابرابرتر و از نظر اجتماعی پراکنده‌تر به وجود می‌آورد (Thomas, 1995: 7). علاوه بر این، نگرانی‌هایی وجود دارد که حریم خصوصی و محرمانه بودن با ظهور یک "جامعۀ نظارت" پیچیده به خطر بیفتد (Lyon, 1994: 12). ترس بزرگ این است که اینترنت «ممکن است به سادگی از طریق کنترل اطلاعات به گسترش کنترل اجتماعی تبدیل شود» (Interrogate the Internet, 1996: 129). بخش‌های بزرگی از جزئیات فردی جوامع به شکل دیجیتالی در پایگاه‌های اطلاعاتی مختلف تبدیل شده‌اند (Mitterer & O'Neill, 1992: 31). آژانس‌هایی از پلیس، ارتش، دولت و صنعت، همه به طور فعال در حال جمع‌آوری و تبادل داده‌های ثبت شدۀ دیجیتالی از طریق فناوری‌های فضای سایبری هستند (Kitchin: 1997: 149).

- جغرافیای سیاسی

از نظر برنت و تیلور «جغرافیای سیاسی مطالعۀ جریان‌های سیاسی است و تنها تفاوت آن با علوم سیاسی، تأکید و توجه آن به آثار و پیامدهای جغرافیایی و به کارگیری فنون تحلیل فضایی است (Burnet & taylor, 1993:19). گلاسنر جغرافیای سیاسی را مطالعۀ روابط موجود میان فعالیت سیاسی انسان و محیط طبیعی او می‌داند (Glassner, 1993:3). جغرافیای سیاسی بخشی از جغرافیاست که به بررسی رابطۀ میان جغرافیا و سیاست می‌پردازد. اینکه چگونه مناسبات قدرت، فضا و مکان را می‌سازند و مکان‌ها و فضاها نقش میانجی سیاست و تعارض را منعکس می‌کنند، در حوزۀ مطالعاتی آن قرار می‌گیرد. در اینجا، تفاوت آن با علوم سیاسی، تأکید و توجه به پیامدهای جغرافیایی و به کارگیری فنون تحلیل فضایی است. میشل پاکیون، جغرافیای سیاسی را پیامدهای جغرافیایی تصمیم‌ها و کنش‌های سیاسی تعریف می‌کند (Pacione, 1985:89). در تعریف دیگری آمده است که جغرافیای سیاسی به عنوان مطالعۀ «کشمکش کنترل، مدیریت زمین و طبیعت» یکی از مباحث دائمی جوامع انسانی است. جغرافیای سیاسی در وسیع‌ترین معنی، مطالعۀ علمی اختلاف‌های منابع مختلف و روش‌های حل اختلاف‌هاست (Blacksell, 2006:1). همچنین جغرافیای سیاسی به مثابه «شکلی از استدلال جغرافیایی» (از یویس لاکاست[1])، «فضایی شدن سیاست جهانی» (ریچارد اشلی)[2] و «انحصار فضایی» (از سیمون دالبی)[3] نیز بیان شده است (O Tuathail, 1996:160). بنابراین، کار جغرافیدانان سیاسی به عنوان فضااندیشان، شناخت و مطالعۀ عناصر بنیادین مربوط به حوزۀ تخصصی خود در فضای جغرافیایی است که بتوانند آنگونه که شایسته و بایسته است بهترین برنامه را جهت به سامان شدن فضای جغرافیایی ارائه دهند و در این راستا جغرافیدانان سیاسی به مطالعه و شناخت از تعامل کنش بُعد سیاسی انسان با فضای جغرافیایی می‌پردازند (قربانی سپهر، ۱۱۷:۱۳۹۷).

[1] Yves Lacoste
[2] Richard Ashley
[3] Simon Dalby

۳. روش تحقیق

روش اصلی پژوهش، با توجه به ماهیت نظری فلسفی و مبتنی بر استدلال‌های منطقی است. بر این اساس، در این پژوهش سعی شده است علاوه بر تصویرسازی آنچه در زمینهٔ فضای سایبر و عملکرد آن در فضای واقعی وجود دارد به تشریح و تبیین مفهوم آن پرداخته شود. همچنین در پژوهش حاضر کوشش شده است تا مفهوم فضای سایبر از بُعد نظری با توجه به نگاشت‌های سایر نظریه‌پردازان پیرامون این موضوع با مفهوم فضا مورد تحلیل و بررسی قرار گیرد. در این راستا برای تبیین و توجیه دلایل سعی شده است با تکیه بر استدلال‌های محکمی از طریق جستجو در پیشینه و تاریخچهٔ شکل‌گیری فضای سایبر و از سوی دیگر ادبیات و مباحث نظری تحقیق نتیجه‌گیری شود. در این پژوهش برای گردآوری و فیش‌برداری آن از اطلاعات کتابخانه‌ای و منابع اینترنتی (مقالات و کتب خارجی) استفاده شده است.

٤. یافته‌های پژوهش

اینترنت یکی از مهم‌ترین اختراعات قرن بیست و یکم است که تأثیر بسزایی در زندگی ما داشته است (Leiner et al., 2009: 25). امروزه اینترنت همهٔ موانع را از بین برده و نحوهٔ ارتباط ما، بازی کردن، کار کردن، خرید کردن، دوست‌یابی، گوش دادن به موسیقی، تماشای فیلم، سفارش غذا، پرداخت قبوض و احوالپرسی با دوستان در تولد و سالگرد آنها را تغییر داده است. دنیای ما به طور فزاینده‌ای شبکه‌ای می‌شود و اطلاعات دیجیتالی شده زیربنای خدمات و زیرساخت‌های کلیدی است (Gallaher et al., 2008: 29).

جغرافیدانان، در حالیکه به وضوح در مطالعهٔ پیامدهای اقتصادی و شهری فناوری‌های فضای سایبر مشارکت دارند، فقط توجه خود را به پیامدهای اجتماعی، فرهنگی و سیاسی فضای سایبر معطوف می‌کنند. کار جامعه‌شناسان، نظریه‌پردازان فرهنگی، مردم‌شناسان و جغرافیدانان نشان داده است که فضای سایبری پرسش‌های جغرافیایی زیادی در ارتباط با هویت، جامعه، دموکراسی، مالکیت، حریم خصوصی و رازداری، و دسترسی و محرومیت دارد. برای این محققان، فناوری‌های فضای سایبری، کاتالیزوری برای تغییر گسترده در فرهنگ هستند (Squire, 1996: 102). از این‌رو، یکی از دلایل اصلی که فضای سایبر توجه این پژوهشگران را به خود جلب می کند، این است که فضای اجتماعی جدیدی از تعامل را فراهم می‌کند، اما فضایی که ماهیت متفاوتی با مفاهیم متعارف و دکارتی از فضا دارد (Kitchin, 1997: 149). فضا در فضای سایبر کاملاً به صورت اجتماعی تولید می‌شود و هیچ همتای فیزیکی و عینی ندارد. بر این بنیان، در ادامه به بررسی مفهوم و قلمرو جغرافیای سیاسی فضای سایبر می-پردازیم؛ زیرا از یک سو حوزهٔ فضای سایبر مهم است و از سوی دیگر دانشی وجود دارد که مفاهیم حوزهٔ فضای سایبر را به صورت تخصصی مورد مطالعه قرار می‌دهد.

- مفهوم جغرافیای سیاسی فضای سایبر

حوزهٔ جغرافیای فضای سایبر نسبتاً جدید است و درست قبل از معرفی اینترنت تجاری در سال ۱۹۹۵ پدیدار شد. با این حال، تعدادی بررسی کلی از فضای سایبر در مفهوم آن به عنوان فضای اینترنت وجود دارد که بر برخی دیدگاه‌ها و ابعاد خاص جغرافیای فضای سایبر تمرکز دارد. نکتهٔ قابل توجه آنکه هیچ مجلهٔ تخصصی مختص جغرافیای فضای سایبر وجود ندارد، به طوریکه مقالاتی در این زمینه عمدتاً در مجلات مرتبط منتشر شده است. نویسندگان آن جغرافیدان نبوده‌اند. بلکه دانشگاهیان علوم فضایی (مثلاً معماران و متخصصان رسانه)، و همچنین دانشمندان سایر رشته ها (فیلسوفان) در مطالعهٔ این موضوع مشارکت داشته‌اند (Kellerman, 2018: 2). اما آن چیز که در ابتدا به نظر می‌رسید اینترنت قرار بود به جغرافیا پایان دهد. اکنون هر کسی، در هر مکانی می‌تواند یک روزنامه، یک موتور جستجو، یک سرویس بازی راه‌اندازی کند و جهان می‌تواند به آن دسترسی داشته باشد.

پس از هزاران سال جغرافیایی که سرنوشت را دیکته می‌کرد، اکنون جهان مسطح است و فرصت‌ها در همه جا به طور مساوی توزیع شده بود. جغرافیای فضای سایبر نسبت به سایر محیط‌ها بسیار تغییرپذیرتر است. جابجایی کوه‌ها و اقیانوس‌ها سخت است، اما بخش‌هایی از فضای سایبر را می‌توان با کلیک یک سوئیچ، روشن و خاموش کرد». جابجایی الکترون‌ها در سراسر کرهٔ زمین ارزان‌تر و سریع‌تر از جابجایی کشتی‌های بزرگ در فواصل طولانی از طریق اصطکاک آب نمک است. لذا کنترل دریا از دسترس بازیگران غیردولتی خارج است. به طور مشابه، در حالیکه بسیاری از بازیگران خصوصی و دولتی در حوزهٔ هوایی وجود دارند، یک کشور همچنان می‌تواند از طریق سرمایه‌گذاری‌های پُرهزینه در جنگنده‌های نسل پنجم و سیستم‌های پشتیبانی ماهواره‌ای به دنبال دستیابی به برتری هوایی باشد (Nye, 2010: 3). در مقابل، موانع ورود در حوزهٔ سایبری به حدی کم است که بازیگران غیردولتی و دولت‌های کوچک می‌توانند نقش مهمی را با هزینه‌ای پایین ایفا کنند. برخلاف دریا، هوا و فضا، «سایبر سه ویژگی مشترک با جنگ زمینی دارد؛ ۱) تعداد بازیکنان، ۲) سهولت ورود و ۳) فرصت پنهان‌سازی (Kramer, 2009: 12).

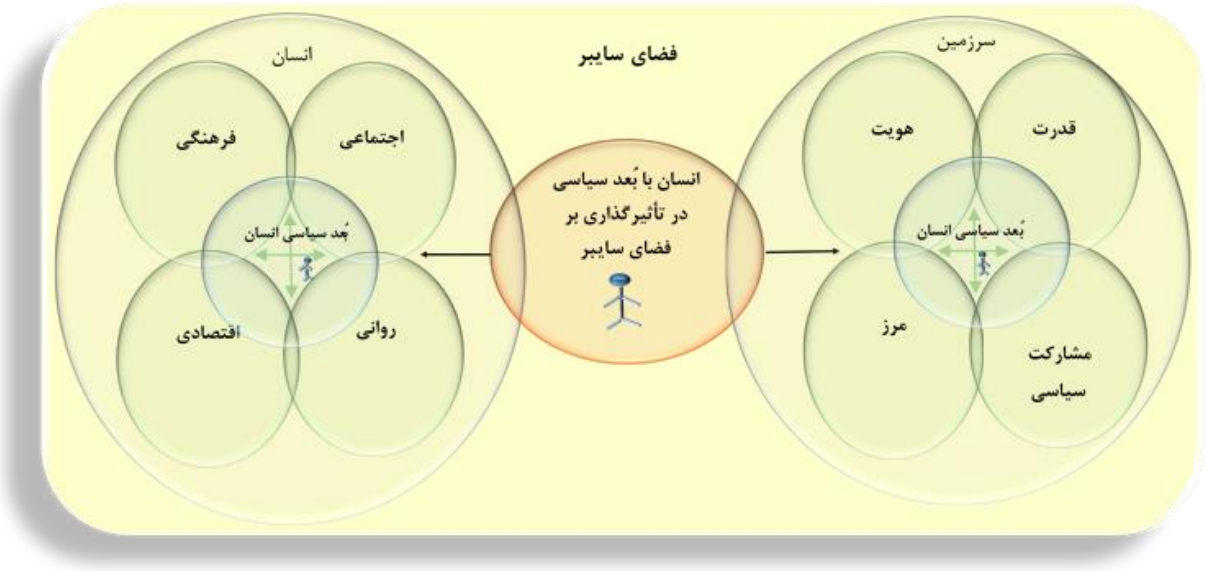
بر این پایه با جدید بودن این موضوع در جهان، در ابتدا لازم است بدانیم منظور ما از جغرافیای سیاسی فضای سایبر چیست. هیچ تعریف عینی و پذیرفته شده‌ای وجود ندارد، بلکه تعاریف کم و بیش خاصی وجود دارد که منعکس کنندهٔ نگرانی‌ها و منافع بازیگران درگیر می‌باشد. مانند چینی‌ها، روس‌ها به ندرت از اصطلاح «فضای سایبری» استفاده می‌کنند، که ممکن است به فضایی جداگانه اشاره کند، فضایی که از مرزها عبور می‌کند، و ترجیح می‌دهند از «اینترنت» یا «امنیت اطلاعات» صحبت کنند، بنابراین بحث را به چیزی برمی‌گردانند که در حیطهٔ فعالیت دولتی است. با این حال، برای اهداف آموزشی، می‌توانیم یک تعریف حداقلی ارائه دهیم. فضای سایبر، فضای ناملموسی که در آن مبادلات بی‌سرزمین شده و بین شهروندان همهٔ ملت‌ها فوراً انجام می‌شود (Douzet, 2014: 2).

در سال ۱۹۹۷، هرودوت در مقاله‌ای با عنوان «اینترنت و جغرافیای سیاسی» گفت: «به نظر می‌رسد اینترنت به جای تأخیر درگیری‌های ژئوپلیتیکی، آنها را تکثیر و پیچیده می‌کند». در مقابل موج صداهای خوش‌بینانه‌ای که چیزی کمتر از پایان جغرافیا را بشارت می‌داد، در آن مقاله به خطرات ژئوپلیتیکی مربوط به گسترش قانع کنندهٔ سیستم های اطلاعاتی و ارتباطی در سراسر جهان اشاره شده است (Douzet, 2014:1). اینترنت به خودی خود موضوع درگیری‌های ژئوپلیتیکی متعدد است که منجر به استراتژی‌های سلطه توسط کشورهایی با منافع متفاوت می‌شود که به دنبال کنترل محتوا، عملکرد و توسعهٔ اقتصادی شبکه هستند. این یک سلاح بسیار استراتژیک برای امنیت ملت ها است و بالاتر از همه ابزاری بسیار قدرتمند در رقابت قدرت بین گروه‌ها، اقلیت‌ها، و نیروهای سیاسی، مذهبی و اقتصادی در سطح محلی و جهانی است (Douzet, 2014:1).

فضای مجازی یک قلمرو به معنای جغرافیایی کلمه، یا «منطقه‌ای نیست که یک گروه انسانی در آن زندگی می‌کند و آن را مالکیت جمعی آن می‌داند» (Douzet, 2014:4)، یا به عنوان یک دولت، «بخشی از فضای زمینی» نیست. با مرزهایش مشخص شده و بر آن اقتدار و صلاحیت خود را اعمال می کند» (Douzet, 2014:4). با این حال، به عنوان فضایی تلقی می‌شود که در آن انسان‌ها، مانند یک قلمرو، در تعامل هستند، برداشتی که آلیکس دسفورجز در مقاله‌اش دربارهٔ بازنمایی‌های فضای سایبر در این موضوع نشان می‌دهد. اما پس از مدتی، اصطلاح «جغرافیای سیاسی فضای سایبری» مجدداً در گفتمان‌های دولتی ظاهر شد، که از دههٔ ۲۰۰۰ آغاز شد، به عنوان سرزمینی برای تسخیر، کنترل، نظارت و تصاحب مجدد، سرزمینی که مرزهای دولتی، حاکمیت و قوانین باید در آن وجود داشته باشد. قابل احترام و بالاتر از همه به عنوان تهدیدی برای امنیت ملی و منافع ملی باشد (Douzet: 2014: 3).

بر این پایه، جغرافیای سیاسی فضای سایبر به موضوع رقابت قدرت میان بازیگران، صحنهٔ تقابل و ابزاری بسیار قدرتمند در نزاع‌های ژئوپلیتیکی تبدیل شده است. با این حال، نزاع‌ها در فضای سایبری قابل تفکیک از رقابت‌های سنتی قدرت ژئوپلیتیک نیست. برعکس، آنها هم بیان و هم بُعد جدیدی از چنین رقابت‌هایی هستند که در همهٔ سطوح تحلیل وجود دارد و باید به عنوان

بخشی از رویکرد چند مقیاسی در نظر گرفته شوند. از این‌رو، مسائل ژئوپلیتیکی فضای سایبر ارتباط تنگاتنگی با ملاحظات سیاسی، اقتصادی، اجتماعی و فرهنگی دارد.



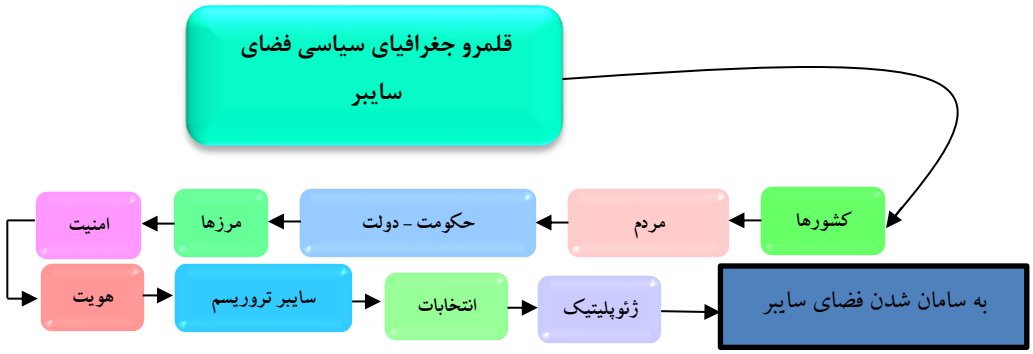
شکل ۱. ماهیت جغرافیای سیاسی فضای سایبر (ترسیم از نگارندگان، ۱۴۰۲)

از آنجا که فضای سایبر به عنوان فضای دوم، شبیه فضای واقعی است، بنابراین بُعد سیاسی دارد. مطالعهٔ بُعد سیاسی فضای [سایبر] موضوع جغرافیای سیاسی فضای مجازی را تشکیل می‌دهد. همانطور که بُعد سیاسی فضای واقعی موضوع علم جغرافیای سیاسی است (حافظ‌نیا ۱۳۹۰: ۴). بر این بنیاد ایفای نقش حکومت‌ها و دولت‌های ملی با فناوری اطلاعات و ارتباطات در فضای سایبر و بازتاب و اثرات آن در فضای جغرافیایی موضوع اصلی جغرافیای سیاسی فضای سایبر می‌باشد که خواه یا ناخواه مفاهیم «قلمرو، مرز، هویت، دولت، ملت و حکومت، امنیت، گفتمان» را که مفاهیم بنیادی جغرافیایی سیاسی است به فضای سایبر منتقل می‌کند و چارچوب آن را مشخص می‌سازد. زمانی که حکومت‌ها وارد این عرصه جهت کنترل و نظارت بر آن شدند جغرافیای سیاسی فضای سایبر در قالب جدید و جدی‌تری مورد توجه قرار گرفت. اساساً وقتی که مفاهیمی چون «ملت، سرزمین و حکومت» در فضای سایبر به کار می‌رود به معنای این می‌باشد که جغرافیای سیاسی فضای سایبر به عنوان یک گرایش جدید و نوظهور می‌تواند این فضا را مورد بررسی قرار دهد. در واقع فضای سایبر سایهٔ فضای واقعی می‌باشد و تمام آن مفاهیم و اصطلاحات جغرافیای سیاسی که در فضای واقعی است، سایهٔ همان در فضای سایبر وجود دارد که روز به روز در حال تکامل، تغییر و دگرگونی است. به هر روی، جغرافیای سیاسی فضای سایبر، از کُنش انسان با بُعد سیاسی بر فضای سایبر شکل می‌گیرد. لذا، جغرافی‌سیاسی‌دانان می‌توانند فضای سایبر را مطالعه و برنامه‌هایی را جهت به سامان شدن این فضا به دولتمردان در راستای [ادارهٔ بهتر آن] ارائه دهند.

- قلمرو جغرافیای سیاسی فضای سایبر

جغرافیدانان خارج از «جهان در سیم» به طور فعال با موضوعات برجستهٔ هویت، جامعه و دموکراسی و نقش‌های مرتبط با فضا و مکان درگیر شده‌اند. با این حال، به طور کلی، جغرافیدانان هنوز باید پیامدهای اجتماعی، فرهنگی و سیاسی فضای مجازی را بررسی کنند و نقش فضا و مکان را در یک فضای اجتماعی پراکنده و فاقد کالبدی بررسی کنند. به این ترتیب، تحقیقات آینده نیاز به پاسخگویی به طیفی از سؤالات مرتبط در مورد توسعهٔ جامعه و آیندهٔ ژئوپلیتیک دارد. این سؤالات عبارتند از: چگونه روابط

فضایی در فضای سایبر حفظ می‌شود، فضای اجتماعی که به عنوان «بی فضا»، «بی مکان» و «عمیقاً ضد فضایی» توصیف شده است (Kitchin, 1998: 389)؟ آیا فضای سایبر مکان را بی معنا می‌کند؟ آیا فضاهای سایبری صرفاً فضاهایی مجسم شده‌اند که در تصاویر و پروتکل‌های دنیای واقعی قرار گرفته‌اند؟ آیا فضای سایبر امکان رمزگذاری مجدد خود را می‌دهد؟ آیا فضای سایبر فضای مؤثری را برای به چالش کشیدن روابط مردم‌سالارانه، همانطور که هاراوی (۱۹۹۱) و همکاران پیشنهاد می‌کنند، فراهم می‌کند؟ آیا رفتار فضایی و اجتماعی در فضاهای سایبری بر رفتار در دنیای واقعی تأثیر می‌گذارد؟ آیا همانطور که راینگولد (۱۹۹۴) می‌گوید، جوامع در فضای سایبر قابل دوام هستند و تا چه اندازه تعاملات اجتماعی با دنیای واقعی متفاوت است؟ فضای سایبر چگونه بر نظام‌های سیاسی مکان‌محور کنونی تأثیر می‌گذارد؟ آیا سیاست های فعلی، همانطور که توسط الکساندر[1] و تو نویان[2] (۱۹۹۶) و (۱۹۹۶) پیشنهاد شده است، با دسترسی به اطلاعات بیشتر و دور زدن دولت‌ها بی‌ثبات می‌شوند؟ آیا مفهوم دولت–ملت در معرض تهدید است؛ زیرا فضای سایبر مرز نمی‌شناسد (Kitchin, 1998: 395)؟ از آنجایی که زیرساخت فیزیکی اینترنت به جغرافیا گره خورده است و دولت‌ها بر فضاهای جغرافیایی حاکم هستند، مکان همچنان به عنوان منبعی در حوزهٔ سایبری اهمیت دارد (Nye, 2010: 5). بر این اساس، جغرافیا علمی است که پیوست نزدیکی به حوزهٔ فضای سایبر دارد؛ زیرا کنش‌های فضای سایبر تأثیر مستقیمی بر محیط‌های جغرافیایی جهان دارد. از جمله کنش‌های فضای سایبر، کنش‌های سیاسی آن بر فضای جغرافیایی است که مبتنی بر تغییر و تحولات عصر کنونی نیاز به آن است که جغرافیای سیاسی به پردازش آن بپردازد تا از تهدیدهای آینده در حوزهٔ سایبری جلوگیری به عمل آورد. در شکل زیر قلمرو جغرافیای سیاسی فضای سایبر ترسیم شده است که می‌تواند حوزهٔ فضای سایبر را در محدودهٔ جغرافیایی سیاسی پوشش دهد.



شکل ۲. قلمرو جغرافیای سیاسی فضای سایبر (ترسیم از نگارندگان، ۱۴۰۲)

تو نگوین و الکساندر (۱۹۹۶) ادعا کردند که فضای سایبری روابط ژئوپلیتیکی را تغییر می‌دهد که منجر به انحلال دولت‌های ملی و سیاست‌های مکان‌محور می‌شود. این ادعاها یا نقش جغرافیا را کاهش می‌دهند یا نشان می‌دهند که روابط فضایی به طور ریشه‌ای پیکربندی می‌شوند. با این حال، هنوز در مورد فضاسازی‌های جدیدی که فضای سایبر ایجاد می‌کند، مطمئن نیستیم. لذا، در تحقیقات آینده به طور مستقیم باید فضاهای مختلف فضای سایبر را بررسی کرد (Kitchin: 1998: 395).

کشورها در طیف وسیعی با مسائل امنیتی مواجه هستند که زمین، هوا و دریا را در برمی‌گیرد. عصر مدرن قلمرو جدیدی به جنگ اضافه کرده است که آن فضای سایبر می‌باشد. جنگ سایبری از طریق فناوری عمل می‌کند و اطلاعات و قدرت را به دولت‌ها و همچنین افراد می‌دهد. به همین دلیل، دولت‌ها باید خود را با تهدیدات جدید وفق دهند. سیاست‌گذاران باید فضای در حال ظهور جنگ را درک کنند و با هوشیاری به آن نزدیک شوند. راه‌حل آسانی نخواهد بود و نیازمند چندین مرحله برای پوشش

[1] Alexander
[2] Thu Nguyen

انواع مختلف حملاتی است که ممکن است رخ دهد. اگرچه فضای سایبر یک جزء مجازی دارد، اما در فضاهای فیزیکی پایه‌گذاری شده است. این بدان معناست که یک استراتژی باید در آن چارچوب تدوین شود (Bordelon: 2016: 5). کشورهای سراسر جهان برای ارتباطات و کنترل دنیای فیزیکی به اندازهٔ کافی به فضای سایبری وابسته شده‌اند. به گونه‌ای که قطعاً جدا شدن از آن غیرممکن است. بنابراین، وظایف و عملکردهای امنیتی هر کشور به طور فزاینده‌ای تحت تأثیر فضای سایبری قرار می‌گیرد (Zhao et al., 2020).

همچنین علاوه بر کشورها، جنبهٔ فیزیکی فضای سایبر، ملت‌ها هستند. مردم ماهیت فضای سایبر را تعیین می‌کنند و ظاهر آن را شکل می‌دهند (Clark, 2010: 3). هر ایده و تکه فناوری که در اینترنت یافت می‌شود محصول ایدهٔ یک فرد است. هیچ بخشی از فضای سایبر وجود ندارد که در ابتدا توسط فردی ایجاد نشده باشد. همچنین با مردم مرتبط است زیرا اگر از فضای سایبری برای حمله استفاده شود، چه علیه یک تجارت دولتی یا خصوصی، مردم هم عامل و هم قربانی هستند. به عنوان مثال، زمانی که یک کسب و کار هک می‌شود و اطلاعات به سرقت می‌رود، آن اطلاعات متعلق به شخصی است. چه او به طور فعال در تجارت شرکت داشته باشد یا نه، آن شخص اکنون درگیر است. مردم تعیین می‌کنند که در حوزهٔ سایبری چه اتفاقی می‌افتد (Bordelon, 2016: 6). با این حال، منابع خارجی وجود دارد که می‌تواند فرد را متقاعد کند که به روش‌های خاصی عمل کند. این منابع را می‌توان در ژئوپلیتیک جستجو کرد. این به این دلیل است که جغرافیا در تعیین اینکه مردم کجا عمل می‌کنند و علیه چه کسی عمل می‌کنند، نقش دارد. یک عامل کلیدی در این پویایی، سیاست است. جغرافیا و سیاست در تعامل هستند و هدف حمله را تعیین می‌کنند (Sheldon, 2014 : 286-288). در اینجا ژئوپلیتیک در فضای سایبر متمرکز شده است.

جنبهٔ دیگر فضای سایبر را دولت‌ها و حکومت‌ها تشکیل می‌دهند. از این‌رو، تحولات و دگرگونی‌های صورت گرفته در جهان و ضرورت و نیاز حکومت‌ها به مدیریت مرزها سبب شده است که، آنها سعی در گسترش و بروز کردن ابزارها و تکنیک‌های مدیریتی و نظارتی خود از طریق فناوری‌های نوین اطلاعاتی و ارتباطی کنند و شکل‌های جدیدی از مدیریت و نظارت بر فضای عینی، فضای مجازی و فضای هویتی (ادراکی) کشور از طریق مدیریت بهینهٔ مرزهای موجود در این فضاها را، شکل داده و گسترش دهند. به عنوان مثال، در اروپا برای مقابله با جرائم مختلف، استفاده از دوربین‌های مداربسته گسترش یافته است. این فناوری توانایی بالایی به حکومت‌ها داده و آنها را قادر کرده است تا بیش از هر زمان دیگر اقدامات و فعالیت گروه‌های سیاسی و جنبش‌های نوین اجتماعی را زیر نظر داشته باشند و در مناطق مرزی عبور و مرور و... را کنترل کنند. تا با استفاده از مدیریت مرزها بتوانند چالش‌ها و مسائل ناشی از تحولات صورت گرفته در فضای سایبر را بر فضای ملی و کشور خود کاهش داده و منافع و امنیت ملی خود و شهروندان خود را از طریق دفاع سایبری تأمین کنند (انصاری و همکاران، ۲۲۹:۱۳۹۷).

در این بین، شکل‌گیری فضای سایبر بر پایهٔ اتصال شبکهٔ جهانی اینترنت، به روشنی گویای این واقعیت است که ویرانگری و آسیب‌رسانی می‌تواند در یک لحظه، سراسر جهان را فراگیرد. سوء استفاده از فناوری‌های رایانه‌ای و اینترنتی می‌تواند امنیت ملی، آسایش عمومی و موجودیت یک جامعه را به مخاطره انداخته و تأثیرهای منفی زیادی بر زندگی افراد اجتماع تحمیل کند. با توسعهٔ رسانه‌های الکترونیکی، در کنار جرائم سنتی یاد شده، فرصت‌های جدیدی برای ایجاد ناامنی از قبیل حملهٔ ویروس‌ها، ورود غیرمجاز به وب‌سایت‌ها و هک کردن آنها، سرقت و سوء استفاده از داده‌ها و ایراد خسارت به رایانه‌ها، در زمرهٔ رفتارهای بزهکارانه‌ای تلقی می‌شوند که قابلیت ارتکاب در محیط خارج از رایانه را ندارند. پیشرفت فناوری رایانه، شرایط و بسترهای مناسبی برای سرقت اطلاعات، تکثیر نرم‌افزارهای غیرمجاز، سوء استفاده از بازار سهام، تجاوز به حقوق مالکیت معنوی و مهم‌تر از همه، تهاجم فرهنگی را فراهم کرده است. با شکل‌گیری فضای سایبر و ورود به عصر اطلاعات و وابستگی‌هایی که در سطوح مختلف فردی تا سطح کشوری به استفاده و ورود به فضای سایبر شکل گرفته است، خیلی از نظریه‌پردازان مدعی از بین رفتن مرز و مرزبندی و همچنین عدم توانایی کنترل و مدیریت مرزی بین کشورها شدند. این اشخاص مرزها را از بین رفته و غیرقابل کنترل

دانسته و سعی در مفهوم‌سازی‌های جدیدی از جمله جهان بدون مرز، دهکدهٔ جهانی و... کردند. نقطهٔ اتکا این اشخاص شکل‌گیری فضای سایبر و آزادی‌های بی حد و حصر در این فضا برای افراد و از بین رفتن کنترل و مدیریت حکومت‌ها در این فضا و همچنین توانایی اثرگذاری و گذر از محدودیت‌های فضای واقعی در این فضا بوده است. اما باید توجه داشت که حکومت‌ها همچنان بر کشورهای خود حاکمیت می‌کنند و قلمرو سرزمینی خود و مرزبندی‌های آن را برای جلوگیری از صدمات و مشکلات ناشی از پیشرفت تکنولوژی به صورت‌های مختلف حفظ می‌کنند (قصری و همکاران، ۱۳۹۰:۳۸۳).

بنابراین، حکومت‌ها دارای اطلاعات دولتی محرمانه در شکل‌های مختلف (مثلاً چاپی، صوتی، الکترونیکی یا تصویری) هستند که به عنوان یک منبع استراتژیک برای اعمال حاکمیت، اتحاد ملی، منافع ملی، اهداف ملی، مدیریت کشور و... می‌باشند. این اطلاعات در عمر حکومت‌ها به گونهٔ مؤثری کنترل و مدیریت می‌شوند و از جایگاه بالایی برای حفظ و نگهداری و امنیت برخوردار هستند. با پیشرفت‌های صورت گرفته در تکنولوژی و افزایش حجم اطلاعات و نیازها برای استفاده از این تکنولوژی در امر نگهداری، جابجایی و... امر حفاظت اطلاعات تمامیت، و محرمانگی اطلاعات دولتی را بیش از پیش به تکنولوژی‌های جدید مانند اینترنت و فضای سایبر وابسته ساخته است. علاوه بر اطلاعات محرمانهٔ حکومتی که می‌تواند به صورت‌های مختلف مورد حمله و تجاوز قرار بگیرد و کشور را با مشکل مواجه سازد، دادن اطلاعات غلط و تهیج کننده به شهروندان و تحت تأثیر قرار دادن آنها برای به دست آوردن منافع خود، زیر سوأل بردن امنیت کشور و شخصیت‌های سیاسی، استفاده از مسائل سیاسی و قومیتی در داخل کشورها و مانور دادن روی آنها به شکل‌های مختلف و تحریک کردن شهروندان کشور بر علیه حکومت و... نام برد. این مسائل به صورت‌های مختلف سبب شده است که حکومت‌ها مرزبندی‌ها و قواعد و قوانین ویژه‌ای برای فضای سایبر تبیین کنند و به صورت‌های مختلف این فضا را از طریق مدیریت مرزهای سایبر مدیریت کنند (همان، ۳۸۴-۳۸۳).

دولت‌های ملی، سازمان‌ها و کاربران نهایی همه نگران تهدیدات محرمانه، یکپارچگی و در دسترس بودن اطلاعات دیجیتالی هستند (Rid & Buchanan, 2015: 31). در دنیای دیجیتالی که به تدریج در هر بخش از زندگی روزمره، چه عمومی و چه خصوصی، نفوذ می‌کند، امنیت یک امر ضروری است. اگر امنیت نباشد دنیا از هم می‌پاشد. حملاتی مانند WannaCry باعث ویرانی شهروندان، مشاغل و سازمان‌های ناآماده شده و عملیات آنها را به خطر انداخته است (Zhu et al, 2011: 385). در حوزهٔ فناوری اطلاعات، امنیت سایبری نقش مهمی ایفا می‌کند. در طول چند دههٔ گذشته، امنیت سایبری پیشرفت کرده است (Ablon & Martin, 2014: 30). وقتی با یک کلاهبرداری مواجه می‌شویم، امنیت سایبری اولین چیزی است که به ذهن می‌رسد. حفاظت از اطلاعات شخصی ما در اینترنت به یک نگرانی بزرگ تبدیل شده است (Dawson & Thomson, 2018: 9). تعداد دستگاه‌های متصل با سرعت زیادی در سال‌های اخیر گسترش یافته است و تا سال ۲۰۲۰ از ۵۰ میلیارد فراتر رفته است. رشد تصاعدی در تعداد دستگاه‌های متصل، پیچیدگی زیرساخت‌های سایبری را افزایش داده و منجر به افزایش تعداد دستگاه‌های آسیب‌پذیر می‌شود (Philip et al, 2014: 330). از آنجایی که "امنیت به داده‌ها مربوط می‌شود"، برای آیندهٔ سیستم‌ها و خدمات امنیت سایبری هوشمند حیاتی است. ما داده‌های امنیتی را در قالب فایل‌ها، گزارش‌ها، بسته‌های شبکه و سایر منابع مرتبط هنگام تلاش برای شناسایی تهدیدات سایبری تجزیه و تحلیل می‌کنیم (Perwej, 2019: 10). هکرها احتمالاً می‌توانند دسترسی غیرمجاز آسانی به اطلاعات پردازش شده با استفاده از فناوری‌های کلان داده (Akhtar et al, 2017: 31) داشته باشند، مگر اینکه تأکید بر دستیابی به امنیت سایبری مؤثر در داده‌های بزرگ (Parwej et al, 2018: 30) باشد. در نتیجه، بدیهی است که کلان داده (Cagri et al, 2018: 2) هم مزایا و هم معایبی دارد. در نتیجه، امنیت سایبری یک نگرانی است که همه را در سراسر جهان تحت تأثیر قرار می‌دهد (Skrjanc et al, 2018: 595).

با توجه به تولید جهانی محصولات نرم‌افزاری و سخت‌افزاری، ارائهٔ گارانتی در فرآیند زنجیرهٔ تأمین محصول غیرممکن است. مقیاس پذیری دامنهٔ سایبری آن را از نظر کیفی متفاوت می‌کند. یک بمب در شدیدترین شرایط، برد فیزیکی محدودی دارد. با این

حال، تهدیدات سایبری طیف بسیار گسترده‌ای از اثرات را دارند، بنابراین ما مکانیزمی داریم که می‌تواند عملیات‌های دنیای واقعی را کنترل کند. مانند بسیاری از حوزه‌های دانش دیگر، عملیات در فضای سایبری توسط تعداد نسبتاً کمی از افراد کنترل می‌شود. کاربران توانایی تغییر یا کنترل نرم‌افزار و سخت‌افزار مورد استفادهٔ خود را ندارند. بر کسی پوشیده نیست که تعداد کمی از مردم می‌توانند به طور مؤثر جنگ سایبری را کنترل یا مدیریت کنند (Zhang et al, 2021: 214).

پنج سناریو را می‌توان برای جنگ سایبری در نظر گرفت: (۱ جاسوسی سایبری تحت حمایت دولت برای جمع‌آوری اطلاعات برای برنامه‌ریزی حملات سایبری آینده، (۲ یک حملهٔ سایبری با هدف ایجاد زمینه برای هر گونه ناآرامی و خیزش مردمی، ۳) حملهٔ سایبری با هدف از کار انداختن تجهیزات و تسهیل تهاجم فیزیکی، (۴ حملهٔ سایبری به عنوان مکمل تهاجم فیزیکی، و (۵ حملهٔ سایبری با هدف تخریب یا اختلال گسترده به عنوان هدف نهایی (جنگ سایبری) (Alibasic et al, 2016). یکی از انواع حملات سایبری رمزگذاری است. رمزگذاری یک روش برگشت‌پذیر برای رمزگذاری داده‌ها است که برای رمزگشایی به یک کلید نیاز دارد. رمزگذاری را می‌توان همراه با رمزگذاری استفاده کرد که سطح دیگری از محرمانگی را فراهم می‌کند (Sun et al, 2018: 50). رمزگذاری عبارت است از پیاده‌سازی و مطالعهٔ رمزگذاری و رمزگشایی داده‌ها به طوریکه تنها توسط افراد خاصی قابل رمزگشایی است. سیستم رمزگذاری و رمزگشایی داده‌ها، سیستم رمزگذاری است (ji et al, 2021: 1280). رمزگذاری ابزاری قدرتمند برای محافظت از اطلاعات مهم و خصوصی در هنگام قرار گرفتن در معرض تهدیدات غریبه‌ها و مجرمان و همچنین برای پنهان کردن فعالیت‌های غیرمجاز از مجریان قانون است. همانطور که کامپیوترها سریعتر رشد می‌کنند و روش‌های خرابی ایمن‌تر می‌شوند، الگوریتم‌های رمزنگاری برای جلوگیری از ناامنی نیاز به یکپارچگی پایدار دارند (Zou et al, 2020: 187). بر این بنیان، سیاست سایبری کشور اکنون بخشی از سیاست امنیت ملی است. حتی اگر سیاست امنیت سایبری یک کشور را همسو با سیاست وزارت خارجه یا سیاست اقتصادی بدانیم، این نوع قوانین و سیاست‌ها به اندازهٔ قانون اساسی حاکمیتی ندارند. در واقع خط مشی در گزارش‌ها و سخنرانی‌ها از طریق بحث در مورد نکات و بحث‌های مختلف ایجاد و منتشر می‌شود. سیاست‌ها برای هدایت و تصمیم‌گیری در مورد قوانین و مقررات ایجاد می‌شوند. خود سیاست مربوط به قوانین و مقررات نیست. در بهترین حالت، قوانین، توافقات و قوانین بیانگر یک سیاست معنادار و عاقلانه است. با این حال، دستورات، قوانین و مقررات اجرایی امنیت سایبری را می‌توان بدون ایجاد خط مشی امنیت سایبری ارائه کرد (Sakhnini et al, 2021).

۵. بحث و نتیجه‌گیری

با توجه به ابهامی که در مورد تعریف (جغرافیای سیاسی فضای سایبر) وجود دارد، تعریفی دقیق و قابل اتکایی در مورد آن ارائه نشده است. از این‌رو، شناخت یک تعریف واحد از (فضای واقعی، فضای مجازی و فضای سایبر و در پیوند آن جغرافیای سیاسی فضای سایبر) نیاز پایه‌ای و اساسی در آیندهٔ علوم جغرافیایی به ویژه جغرافیای سیاسی در کنار سایر علوم است. در ادامه سعی نگارندگان بر آن است که تعریفی شفاف، ساده و قابل فهم از جغرافیای سیاسی فضای سایبر ارائه دهند تا بلکه به صورت دقیق‌تر مورد بحث و بررسی قرار گیرد.

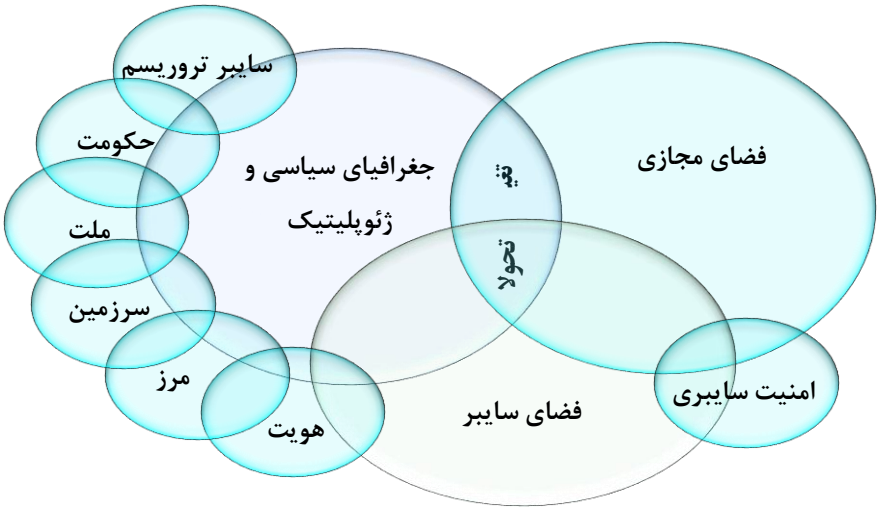
فضای واقعی همان فضای جغرافیایی: فضای جغرافیایی شبکه‌ای درهم‌تنیده از پدیده‌های طبیعت‌ساخت و پدیده‌های انسان-ساخت است که جمعی در آن زندگی می‌کنند و فقط با فلسفه‌اندیشی در جغرافیاست که می‌توان فضای جغرافیایی را شناخت و درک نمود. بر این اساس کاری که جغرافیدانان به عنوان (دانندِگانِ فضای جغرافیایی) انجام می‌دهند، شناخت و مطالعهٔ فضای جغرافیایی و به طور بایسته‌تر زیست جهان[1] در مقیاس‌های (محلی، ملی، منطقه‌ای و جهانی) است.

---

[1]. هایدیگر حضور در عالم را عین حقیقت وجود انسان (Dasein) می‌داند. نحوهٔ وجود آدمی [بودن- در- جهان (Being- in- the- world)] است (حقیقت، ۱۳۹۴:۳۸۱). «زیست جهان» به مثابه یکی از عناصر کلیدی «کُنش ارتباطی»[1] وسیله‌ای است که از طریق کُنش آن کُنش ارتباطی در سه جهان «طبیعت، جامعه و خود» تحقق

فضای مجازی: فضای مجازی، فضایی است که در آن یک شخص با دنیایی به غیر از دنیای خود ارتباط مستقیم ندارد و به فضای شخصی خود در صفحهٔ کامپیوتر محدود می‌شود. به عبارتی فضای مجازی زمانی است که از سیستم شخصی خود جهت بازی یا سایر کارها به صورت آفلاین استفاده می‌کنیم. لذا، در آن زمان به اینترنت وصل نیستیم و اثرگذاری متقابلی وجود نخواهد داشت. در واقع فضای مجازی فضایی است که در صفحهٔ مجازی اتفاق می‌افتد ولی بدون استفاده از اینترنت و داده‌های اتصالی.

فضای سایبر: فضای سایبر در برگیرنده زیرساخت‌های ارتباطی، ارتباطات و تعامل است و در حقیقت بین دو نفر ارتباط برقرار می‌شود و در واقع اثرگذاری دو سویه با فضای واقعی دارد. لذا می‌توان اینگونه تعبیر نمود که فضای سایبر، عرصه‌ای است که در آن جهان به مثابه دهکده‌ای کوچک واقع شده است و شکل‌گیری آن منجر به تحولات عظیم بر سایر فضاهای جغرافیایی گذاشته است و در قرن بیست و یکم خود را به عنوان یک فضای جهانی قابل دسترس برای همگان مطرح کرده و در تمامی سطوح فضاها کاربرد دارد. به بیان دیگری فضای سایبر، فضاییست که کنش‌های ارتباطی را در زیست جهان سهل و آسان نموده و اثرگذاری روزافزونی بر فضای زندگی ساکنان جهان در عصر حاضر دارد. به طوریکه اگر اندک زمانی پای از این گوی خاکی برکنیم و از بالا به آن بنگریم خواهیم دید که کدامین بوم‌ها متأثر از فضای سایبر توسعه یافته و به بالندگی رسیده‌اند و کدامین بوم‌ها تأثیر خاصی نپذیرفته و ناکام مانده‌اند به عبارت دیگر کامیابی و ناکامی بوم‌ها در قرن حاضر بستگی زیادی به بهره‌گیری از فناوری‌های ارتباطی- اطلاعاتی (فضای سایبر) دارد.



شکل ۳. درهم‌تنیدگی فضاها در یکدیگر

بنابراین؛ از پیوند این سه فضا، جغرافیای سیاسی فضای سایبر نمود می‌یابد و قلمرو آن شکل می‌گیرد. از این‌رو، فضای سایبر نقش اساسی و بنیادینی در شکل‌دهی به آگاهی و مشارکت ملت‌ها در تعیین سرنوشتشان داشته است. بر این اساس نیاز به آن است که دولت‌ها نسبت به فضای سایبر شناخت لازم را پیدا کرده و با کارکردهای نوین آن آشنا شوند تا آنگونه که شایسته است شهروندان در مشارکت سیاسی به خصوص در عرصهٔ انتخابات از آن بهره‌مند گردند و از سوی دیگر بتوانند با حملات سایبری که امنیت کشور را دچار تهدید می‌کند، مقابله کنند و امنیت سایبری را تأمین کنند. بر این بنیاد، جغرافیای سیاسی فضای سایبر، از کُنش انسان با بُعد سیاسی بر فضای سایبر شکل می‌گیرد. بنابراین، جغرافی‌سیاسی‌دانان می‌توانند فضای سایبر را مطالعه و برنامه‌هایی را جهت به سامان شدن این فضا به دولتمردان در راستای [ادارهٔ بهتر آن] ارائه دهند.

می‌یابد (TCA, 1987: 119). در نهایت زیست امری است انسانی یعنی زیست جهان یک حوزهٔ انسانی است به خاطر وضعیت انسان در این جهان.

به هر روی، فضای سایبر و فناوری‌های مرتبط یکی از مهم‌ترین منابع قدرت در هزارهٔ سوم است. از این‌رو، فضای سایبر یکی از مؤلفه‌های قدرت‌زای ژئوپلیتیکی برای کشورها محسوب می‌شود؛ به‌طوری که امروزه کشورهای قدرتمند با بهره‌گیری از ظرفیت-های فضای سایبر بر دیگر کشورها تأثیر می‌گذارند. به‌طور مثال یک کشور با بهره‌گیری از این فضا، در انتخابات کشور دیگر تداخل ایجاد می‌کند و سرنوشت سیاسی آن کشور را مورد تهدید قرار می‌دهد و یا بازیگران قدرتمند با استفاده از این فضا به مکان‌ها حساس کشورهای رقیب نفوذ کرده و تهدید جدی برای آن کشور ایجاد می‌کند؛ بر این اساس، با قابلیت‌های موجد در فضای سایبر این فضا به مباحث جغرافیای سیاسی و ژئوپلیتیک وارد شده است؛ زیرا این فضا به خودی خود همهٔ مفاهیم موجود در جغرافیای سیاسی که در فضای حقیقی مورد مطالعه قرار می‌دهد را در فضای سایبر در برگرفته است و نیاز است که به صورت علمی تمام جنبه‌های مرتبط با این علم در حوزهٔ فضای سایبر بررسی شود تا بتوان از تهدیدهای آینده برای کشورها جلوگیری به عمل آورد و از سوی دیگر بتوان قابلیت‌های این فضا را به درستی در جهت نظم جهانی مدیریت کرد.

منابع

۱. انصاری، ز.، حسین پور مطلق، م.، و قربانی سپهر، آ. (۱۳۹۷). دیدگاهی نوین به مشارکت سیاسی (با تأکید بر نقش فضای سایبر در انتخابات ریاست جمهوری دوره دوازدهم). تهران، انجمن ژئوپلیتیک ایران.

۲. حافظ‌نیا، م. ر. (۱۳۹۰). جغرافیای سیاسی فضای مجازی، تهران: انتشارات سمت.

۳. حافظ‌نیا، م. ر.، و کاویانی راد، م. (۱۳۹۳). فلسفه جغرافیای سیاسی. تهران، انتشارات پژوهشکده مطالعات راهبردی.

۴. حقیقت، س. ص. (۱۳۹۴). روش‌شناسی علوم سیاسی. قم: انتشارات دانشگاه مفید.

۵. رحیمی، ح. ا. (۱۳۹۵). برنامه‌ریزی فضایی با رویکرد پویش ساختاری – کارکردی: به سوی پیوند جبرگرایی فضایی با انسان-گرایی، فصلنامهٔ برنامه‌ریزی و آمایش فضا، ۲۰(۴)، ۱۱۴-۹۱. URL: http://hsmsp.modares.ac.ir/article-۲۱-۷۲۵۴-fa.html

۶. قربانی سپهر، آ. (۱۳۹۷). تبیین مفهوم و قلمرو جغرافیای سیاسی فضای شهری، پایان نامه کارشناسی ارشد، به راهنمایی محسن جان پرور، دانشگاه فردوسی مشهد.

۷. قربانی سپهر، آ.، و انصاری، ز. (۱۳۹۷). نقش و جایگاه فضای سایبر در توسعه کشور به عنوان الگویی راهبردی. تهران، دوازدهمین کنگره پیشگامان پیشرفت ایران اسلامی.

۸. قصری، م.، جان پرور، م.، و حیدری، ط. (۱۳۹۰). مدیریت مرزهای فضای سایبر، گام نخست دفاع سایبری"، مجموعه مقالات نخستین همایش ملی دفاع سایبری.

۹. منوچهری میاندوآب، ا.، رهنمایی، م. ت. (۱۳۹۸). تحلیلی بر فرایند تولید فضای سرمایه‌داری دولتی در ایران مورد: شهر تهران، فصلنامهٔ برنامه‌ریزی و آمایش فضا، ۲۳(۱)، ۱۱۶-۸۵. 20.1001.1.16059689.1398.23.1.5.6.

10. Ablon, L., Martin, C. (2014). Libicki and Andrea A. Golay, Markets for Cybercnme Tools and Stolen Data: Hackers, Bazaar, 1-85.
11. Aghajani, G., Ghadimi, N., 2018. Multi-objective energy management in a micro-grid, Energy Rep, 4, 218–225.
12. Akhtar, N., Parwej, F. Perwej, Y. (2017). A Perusal of Big Data Classification and Hadoop Technology, International Transaction of Electrical and Computer Engineers System (ITECES), USA, 4 (1), 26-38. DOI: 10.12691/iteces-4-1-4.
13. Alibasic, A., et al. (2016). Cybersecurity for smart cities: A brief review. In: Nternational Workshop on Data Analytics for Renewable Energy Integration. Springer.
14. Ansari, Z., Hosseinpour Motlagh, M., and Ghorbani Sepehr, A. (2017). A new perspective on political participation (with an emphasis on the role of cyberspace in the 12th presidential election). Tehran, Geopolitical Association of Iran. (In Persian).
15. Autio, E. (2017). Digitalisation, Ecosystems, Entrepreneurship and Policy.

16. Blacksell, M. (2006). Political Geography, London and New York: Routledge.
17. Bordelon, E. B. (2016). Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law. Cyber War and Geopolitics in the Honors Program Liberty University, 22(3), 1-30.
18. Bordelon, E. B. (2016). Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law. Cyber War and Geopolitics in the Honors Program Liberty University, 22(3), 1-30.
19. Bronson, K. (2019). Looking through a responsible innovation lens at uneven engagements with digital farming. NJAS Wageningen J. Life Sci. 90–91, 100-294 https://doi.org/10.1016/J.NJAS.2019.03.001.
20. Brunet, R. (1996). Building Models for Spatial Analysis, special issue in English, geography and anthology, CNRS, Paris, 1996.
21. Burnett, A. D. and Taylor. P. J. (1993). Political Geography, London Publishing longman Group.
22. Cagri, B A., Rahime, B. S., and Shujun, L. (2018). Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an example, SMSociety.
23. Clark, D. D. (2010). Characterizing Cyberspace: Past, present and future, Characterizing cyberspace: Past, present and future (ECIR Working Paper No. 2010-3). MIT Political Science Department. Version: Author's final manuscript.
24. Dawson, J. and Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance, Frontiers in Psychology, 9(JUN), 1–12. doi:10.3389/fpsyg.2018.0074.
25. Douzet, F. (2014). Understanding Cyberspace with Geopolitics, In Hérodote, 1 (152), 3-21, Translated from the French by JPD Systems.
26. Gallaher, M. Link, A., and Rowe, B. (2008). Cyber Security: Economic Strategies and Public Policy Alternatives, Edward Elgar Publishing.
27. Ghorbani Sepehr, A. (2017). Explaining the concept and scope of the political geography of urban space, master's thesis, under the guidance of Mohsen Jan Peror, Ferdowsi University of Mashhad.
28. Ghorbani Sepehr, A., and Ansari, Z. (2017). The role and place of cyberspace in the country's development as a strategic model. Tehran, the 12th Congress of Pioneers of Islamic Iran's Progress. (In Persian).
29. Glassner, M. I. (1993). Political Geography, New York: John wiley and Sons.
30. Hafeznia, M. R. (2011). Political Geography of Virtual Space. Tehran, Samt Publications. (In Persian).
31. Hafeznia, M. R., and Kaviyani Rad, M. (2014). Philosophy of political geography. Tehran, Strategic Studies Research Institute Publications. (In Persian).
32. Haghigat, S. S. (2014). Political science methodology. Qom: Mofid University Press. (In Persian).
33. Hillier, B and Hanson, J. (1984). The Social logic of Space, Cambridge Univercity Press, Cambridge.
34. Interrogate the Internet. (1996). Contradictions in cyberspace: collective response. In Shields, R., editor, Cultures of Internet: virtual spaces, real histories and living bodies, London: Sage.
35. Jedrej, M.C. (2000). Time and Space, in Barnard, A. Spencer, Jonathan.
36. ji, Z., et al. (2021). Harmonizing safety and security risk analysis and prevention in cyber–physical systems. Process Saf. Environ. Prot. 148, 1279–1291.
37. Judge, M.A., et al. (2021). Price-based demand response for household load management with interval uncertainty. Energy Rep.
38. Kellerman, A. (2018). Geography of Cyberspace, LAST MODIFIED. DOI: 10.1093/OBO/9780199874002-0190.
39. Kitchin, R. and Thrift, N (2009). International Encyclopedia of Human Geography. Uk: Elsevier.
40. Kitchin, R. M. (1998). Towards geographies of cyberspace. Progress in Human Geography, 22(3), 385-406.
41. Kitchin, R. M. (1998). Towards geographies of cyberspace. Progress in Human Geography, 22(3), 385-406.
42. Kitchin, R.M. (1997). Social transformations through spatial transformations: from `geospace' to `cyberspaces'. In Behar, J., editor, Sociological studies of telecommunications, computerization and cyberspace, New York: Dowling College Press.
43. Kramer, F. (2009). Cyberpower and National Security, in Kramer, cited.
44. Leiner, B. M., et. al. (2009). A Brief History of the Internet, ACM SIGCOMM Computer Communication Review, 39 (5), 22-31. http://doi.acm.org/10.1145/1629607.1629613.
45. Li, A., Zhao, P., He, H., Mansourian, A., & Axhausen, K. W. (2021). How did micro- mobility change in response to Covid-19 pandemic? A case study based on spatial- temporal-semantic analytics. Computers, Environment and Urban Systems, 90, Article 101703.
46. Li, N., et al. (2020). Early validation of cyber–physical space systems via multi-concerns integration. J. Syst. Softw. 170.
47. Lyon, D. (1994). The electronic eye: the rise of the surveillance society. Oxford: Polity Press.
48. Maigron, P. (2020). World - autonomous system number statistics - sorted by number.
49. Manouchehri Miandoab, A., rahnemaie, M. T. (2019) an analysis of the process of producing the state capitalist space in Iran, Case Study: Tehran City. The Journal of Spatial Planning, 23 (1), 85-116. URL: http://hsmsp.modares.ac.ir/article-21-25111-fa.html. (In Persian).

50. Mejias, U.A., Couldry, N. (2019). Datafication. https://policyreview.info.
51. Mitterer, J. and O'Neill, K. (1992). The end of `information': computers, democracy and the university.
52. Nye, J. (2010). Cyber Power, Harvard Kennedy School, Cambridge.
53. O Tuathail, G. (1996). Critical Geopolitics: the political of writing global space, London, Routledge.
54. Pacione, M. (1985). Progress in Political Geography, Publication of London, Croom Helm.
55. Park, K. (2005). The internet as a complex system. In: The Internet as a Large-Scale Complex System.
56. Parwej, F., Nikhat, A., Perwej, Y. (2018). A Close-Up View About Spark in Big Data Jurisdiction", International Journal of Engineering Research and Application (IJERA), ISSN: 2248-9622, 8 (1), 26-41. DOI: 10.9790/9622-0801022641.
57. Perwej, Y. (2019). The Hadoop Security in Big Data: A Technological Viewpoint and Analysis, International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE), E-ISSN: 2320-7639, 7 (3), 1- 14. DOI: 10.26438/ijsrcse/v7i3.1014.
58. Philip, C. L., Chen, Q. and Zhang, C. Y. (2014). "Data-intensive applications challenges techniques and technologies: A survey on big data", Information Sciences, vol. 275, pp. 314-347.
59. Prause, L., Hingley, M., Luis Vilalta-Perdomo, E. (2021). Digital agriculture and labor: a few challenges for social sustainability. Sustainability 13 (11), 59-80. https://doi. org/10.3390/SU13115980.
60. Qasri, M., Jan Prover, M., and Heydari, T. (2011). Management of cyber space boundaries, the first step of cyber defense", Proceedings of the First National Cyber Defense Conference. (In Persian).
61. Rahimi, H. (2016). Tructural-Functional Dynamics Approach to Spatial Planning: toward Linking Spatial Determinism with Humanism. The Journal of Spatial Planning, 20(4), 91-114. http://hsmsp.modares.ac.ir/article-21-7254-fa.html. (In Persian).
62. Rid, T. and Buchanan, B. (2015). Attributing cyber-attacks", Journal of Strate St., 38 (1), 4-37.
63. Rijswijk, K., Klerkx, L., Bacco, M., Bartolini, F., Bulten, E., Debruyne, L., Dessein, J., Scotti, I., Brunori, G. (2021). Digital transformation of agriculture and rural areas: a socio-cyber-physical system framework to support responsibilisation. J. Rural. Stud. 85, 79–90. https://doi.org/10.1016/J.JRURSTUD.2021.05.003.
64. Rose, D.C., Lyon, J., de Boon, A., Hanheide, M., Pearson, S. (2021). Responsible development of autonomous robotics in agriculture. Nat. Food 2 (5), 306–309. https://doi.org/10.1038/s43016-021-00287-9.
65. Sakhnini, J., et al. (2021). Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. Phys. Commun. 47.
66. Sheldon, J. B. (2014). Geopolitics and Cyber Power: Why Geography Still Matters," American Foreign Policy Interests, 36 (5), 286-288.
67. Skrjanc, I., Ozawa, S. Ban, T. and Dovzan, D. (2018). Large-scale cyber-attacks monitoring using Evolving CauchyPossibilistic Clustering, in Applied Soft Computing, Elsevier, 62, 592-601.
68. Soja, E. (1990). Postmodern geographies, reassertion of space in critical social theory, Verso, second expression, London.
69. Sparrow, R., Howard, M. (2021). Robots in agriculture: prospects, impacts, ethics, and policy. Precis. Agric. 22 (3), 818–833. https://doi.org/10.1007/s11119-020-09757- 9.
70. Squire, S.J. (1996). Re-territorializing knowledge(s): electronic spaces and virtual geographies. Area 28, 101-103.
71. Sun,C.-C., Hahn, A., Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. Int. J. Electr. Power Energy Syst. 99, 45–56.
72. Tan, S., et al. (2021). Attack detection design for dc microgrid using eigenvalue assignment approach. Energy Rep. 7, 469–476.
73. The Theory of Communicative Action. (1987). Life world and system: a critque of functionalist reason, trans by: Thomas Mccarthy. vol. 2. Boston: Beacon Press.
74. Thomas, R. (1995). Access and inequality. In Heap, N., Thomas, R., Einon, G., Mason, R. and MacKay, H., editors, Information technology and society: a reader, Milton Keynes: Open University Press.
75. Thomson, J.R. (2015). Cyber security, cyber-attack and cyber-espionage. In: Thomson, J.R. (Ed.), High Integrity Systems and Safety Management in Hazardous Industries. Butterworth-Heinemann, Boston, 45–53.
76. van Dijck, J. (2014). Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. Surveill. Soc. 12 (2), 197–208. https://doi.org/10.24908/ss. v12i2.4776.
77. Vial, G. (2019). Understanding digital transformation: a review and a research agenda. J. Strateg. Inf. Syst. 28 (2), 118–144. https://doi.org/10.1016/J.JSIS.2019.01.003.
78. W. Stallings, R.V. (2001). Slyke, Business Data Communication, Upper Saddle River, 4th ed., New Jersey, USA: Prentice-Hall.
79. Zhang, X., et al. (2021). Ensuring confidentiality and availability of sensitive data over a network system under cyber threats. Reliab. Eng. Syst. Saf. 214, 107697.
80. Zhao, J., et al. (2020). TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Comput. Secur. 95, 101867.

81. Zhu, B. Joseph, A. and Sastry, S. (2011). A taxonomy of cyber-attacks on SCADA systems, 2011 International conference on internet of things and 4th international conference on cyber physical and social computing, 380-388.
82. Zou, T., et al. (2020). Smart grids cyber–physical security: Parameter correction model against unbalanced false data injection attacks. Electr. Power Syst. Res. 187, 106490.